

**UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE**

IN RE GOOGLE INC. COOKIE
PLACEMENT CONSUMER PRIVACY
LITIGATION

Case No. 12-MD-2358 (SLR)

This Document Relates to:
All Actions

**PLAINTIFFS' BRIEF IN OPPOSITION TO
DEFENDANT GOOGLE INC.'S MOTION TO DISMISS**

KEEFE BARTELS, LLC

Stephen G. Grygiel (Del Bar No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefebartels.com

Executive Committee Member

**BARTIMUS, FRICKLETON,
ROBERTSON & GORNY, P.C.**

James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertson, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

[Additional Counsel on Signature Page]

Dated: March 29, 2013

STRANGE & CARPENTER

Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

STEWARTS LAW US LLP

Ralph N. Sianni (Del Bar No. 4151)
Michele S. Carino (Del Bar. No. 5576)
Lydia E. York (Del Bar No. 5584)
I.M. Pei Building
1105 North Market Street, Suite 2000
Wilmington, DE 19801
Tel: 302-298-1200
rsianni@stewartslaw.com

*Plaintiffs' Steering Committee Member and
Liaison Counsel*

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
I. NATURE AND STAGE OF THE PROCEEDINGS	1
II. SUMMARY OF ARGUMENT	1
III. CONTESTED AND UNSUPPORTED “FACTS” REQUIRE DISCOVERY.....	1
A. The Complaint’s Facts, Not Google’s, Control	1
B. Google’s Cookies Permit User Tracking and Information Collection.....	3
C. Google’s “Facts” are Unsupported or Contested.....	4
D. Plaintiffs Allege Personal and Direct Harm.....	7
IV. PLAINTIFFS HAVE PROPERLY ALLEGED STANDING.....	8
A. Plaintiffs Need Only Allege, Not Prove, “Identifiable Trifle” of Harm.....	8
B. Plaintiffs Do Allege Personalized Harm.....	9
C. Plaintiffs Properly Allege Statutory Standing.....	10
D. Google’s Cited Cases Do Not Support Google’s Standing Argument	12
V. LEGAL ARGUMENTS.....	13
A. Count I – The Complaint States A Claim Under The Electronic Communications Privacy Act (“ECPA”), 18. U.S.C. § 2510 Et Seq.....	13
1. Google Was Not a Party to the Communication; It May Not Manufacture a Statutory Exception Through Its Own Illegal Conduct	14
2. Google Did Not Have Prior Consent from a Party to the Communication.....	15
3. Google Intercepted the “Content” of Communications	16
4. The Complaint’s Facts Showing Improper Interception Authorize Use and Disclosure Allegations.	18
B. COUNT II - PLAINTIFFS HAVE PLED A CAUSE OF ACTION UNDER THE STORED COMMUNICATIONS ACT (“SCA”).....	18
1. Google Accessed Information in “Electronic Storage”	19
2. Browser-Managed Files on Computer and Mobile Devices are “Facilities” Under the SCA.....	20

3.	Google’s Access Was Not Authorized	23
C.	COUNT III - PLAINTIFFS HAVE STATED A CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT (“CFAA”)	23
1.	Plaintiffs Have Alleged Sufficient Damage or Loss.....	24
2.	Plaintiffs Allege Sufficient Facts To Support Their CFAA Claim.....	26
a.	Plaintiffs Have Alleged Both Transmission Offense and Unauthorized Access Offense.....	26
D.	COUNTS IV & V - PLAINTIFFS HAVE PROPERLY PLED CAUSES OF ACTION FOR INVASION OF PRIVACY & INTRUSION ON SECLUSION ..	27
E.	COUNT VI - PLAINTIFFS HAVE PROPERLY PLED A CALIFORNIA UNFAIR COMPETITION LAW CLAIM (“UCL”)	28
F.	COUNT VII - PLAINTIFFS STATE A CLAIM UNDER PENAL CODE § 502 (COMPREHENSIVE COMPUTER DATA ACCESS & FRAUD ACT).....	30
1.	The Complaint Alleges that Google Placed Cookies on the Plaintiffs’ Computers Without Permission	31
2.	The Complaint Alleges that Google’s Cookies are Contaminants.....	31
3.	Damages and Losses.....	31
G.	COUNT VIII - PLAINTIFFS HAVE PLED A CAUSE OF ACTION UNDER THE CALIFORNIA WIRETAP ACT.....	32
H.	COUNT IX - PLAINTIFFS HAVE STATED A CLAIM UNDER THE CONSUMERS LEGAL REMEDIES ACT (“CLRA”)	33
VI.	CONCLUSION.....	35

TABLE OF AUTHORITIES

CASES

<i>Alston v. Countrywide Fin. Corp.</i> , 585 F.3d 753 (3d Cir. 2009).....	10, 11
<i>In re Apple & AT&TM Antitrust Litig.</i> , 596 F. Supp. 2d 1288 (N.D. Cal. 2008)	25
<i>In re Application of the United States for an Order Authorizing the Use of a Pen Register and Trap</i> , 396 F. Supp. 2d 45 (D. Mass. 2005)	17
<i>Bagramian v. Legal Recovery Law Offices, Inc.</i> , No. CV 12-1512-CAS (CAS) (MRWx), 2013 WL 550490 (C.D. Cal. Feb. 11, 2013).....	15
<i>Bartnicki v. Vopper</i> , 200 F.3d 109 (3d Cir. 1999).....	18
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	2, 3, 9, 26
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997).....	12
<i>Bowman v. Wilson</i> , 672 F.2d 1145 (3d Cir. 1982).....	8
<i>In re Ins. Brokerage Antitrust Litig.</i> , 579 F.3d 241 (3d Cir. 2009).....	8
<i>Brown v. Waddell</i> , 50 F.3d 285 (4th Cir. 1995)	17
<i>Cel-Tech Commc’ns., Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal. 4th 163 (1999)	29
<i>Chance v. Avenue A, Inc.</i> , 165 F.Supp.2d 1153 (W.D. Wash. 2001).....	22
<i>Clapper v. Amnesty Int’l. USA</i> , 133 S.Ct. 1138 (Feb. 26, 2013).....	9
<i>Claridge v. RockYou</i> , 785 F. Supp. 2d 855 (N.D. Cal. 2011)	10

<i>Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz</i> , 793 F. Supp. 2d 311 (D.D.C. 2011)	21
<i>Cousineau v. Microsoft Corp.</i> , No. C11-1438-JCC (W.D. Wash. June 22, 2012).....	22
<i>Crispin v. Christian Audiger, Inc.</i> , 717 F. Supp. 2d 965 (C.D. Cal. 2010)	19
<i>Danvers Motor Co., Inc. v. Ford Motor Co.</i> , 432 F.3d 286 (3d Cir. 2005).....	9
<i>Del Vecchio v. Amazon.com Inc.</i> , No. 11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011).....	12, 13, 30
<i>Doe I, et al. v. AOL LLC</i> , 719 F. Supp. 2d 1102 (N.D. Cal. 2010)	34
<i>In re Doubleclick Privacy Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y.2001).....	<i>passim</i>
<i>Edwards v. First Am. Corp.</i> , 610 F.3d 514 (9th Cir. 2020)	11
<i>Expert Janitorial LLC v. Williams</i> , 2010 WL 908740 (E.D. Tenn. Mar. 12, 2010)	19, 22
<i>In re Facebook Privacy Litigation</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011)	14
<i>Fellner v. Tri-Union Seafoods, L.L.C.</i> 539 F.3d 237 (3d. Cir. 2008).....	28
<i>Ferrington v. McAfee, Inc.</i> , 2010 WL 3910169 (N.D. Cal. Oct. 5, 2010).....	33
<i>Fraley v. Facebook, Inc.</i> , 830 F. Supp. 2d 785 (N.D. Cal. 2011)	30
<i>Freedom Banc Mortg. Servs., Inc. v. O’Harra</i> , No. 2:11-CV-01073, 2012 WL 3862209 (S.D. Ohio Sept. 5, 2012)	20
<i>Garcia v. City of Laredo</i> , 702 F.3d 788 (5th Cir. 2012)	20, 22

<i>Gaos v. Google</i> , No. 5:10-CV-4809, 2012 WL 10964646, (N.D. Cal. Mar. 29, 2012)	11
<i>In re Global Indus. Tech., Inc.</i> , 645 F.3d 201 (3d Cir. 2011).....	8
<i>Golod v. Bank of Am. Corp.</i> , Civil No. 08-746 (NLH) (AMD), 2009 WL 1605309 (D. Del. June 4, 2009).....	3, 19
<i>In re Google, Inc. Privacy Policy Litig.</i> , No. C 12-01382 PSG, 2012 WL 6738343	12
<i>In re Google Inc. St. View Electronic Commc'ns Litig.</i> , 794 F. Supp. 2d 1067 (N.D. Cal. 2011)	28
<i>Hauk v. JPMorgan Chase Bank USA</i> , 552 F.3d 1114 (9th Cir. 2009)	28
<i>Hepting v. AT&T Corp.</i> , 439 F. Supp. 2d 974 (N.D. Cal. 2006)	29
<i>Hill v. Nat'l Collegiate Athletic Ass'n</i> , 7 Cal. 4th 1 (1994)	27
<i>In re Intuit Privacy Litig.</i> , 138 F.Supp.2d 1272 (C.D. Cal. 2001).....	19, 22
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	14
<i>In re iPhone Application Litig.</i> , No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).....	30, 31, 33
<i>Kasky v. Nike, Inc.</i> , 27 Cal. 4th 939 (2002)	28
<i>Kearney v. Salomon Smith Barney, Inc.</i> , 39 Cal. 4th 95 (Cal. 2006).....	32
<i>Khoday v. Symantec Corp.</i> , 858 F. Supp. 2d 1004 (D. Minn. 2012).....	33
<i>Krottner v. Starbucks Corp.</i> , 628 F.3d 1139 (9th Cir. 2010)	30

<i>LaCourt v. Specific Media, Inc.</i> , No. SACV10-1256, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)	12
<i>Leonard v. Stemtech Int’l, Inc.</i> Civ. Action No. 12-86-LPS-CJB, 2012 WL 3655512 (D. Del. Aug. 24, 2012).....	5
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	8, 10, 12
<i>Lujan v. Nat’l Wildlife Fed.</i> , 497 U.S. 871 (1990).....	8
<i>Marion v. TDI, Inc.</i> , 591 F.3d 137 (3d Cir. 2010).....	9
<i>Maya v. Centex</i> , 658 F.3d 1060 (9th Cir. 2011)	9
<i>McNair v. Synopse Grp., Inc.</i> , 672 F.3d 213 (3d Cir. 2012).....	10
<i>Motors, Inc. v. Times Mirror Co.</i> , 102 Cal. App. 3d 735 (1980)	29
<i>Motschenbacher v. R. J. Reynolds Tobacco Co.</i> , 498 F.2d 821 (9th Cir 1974)	34
<i>Nexsales Corp. v. Salebuild, Inc.</i> , No. C-11-3915 EMC, 2012 WL 216260 (N.D. Cal. Jan. 24, 2012)	32
<i>Oracle Am., Inc., v. Service Key, LLC</i> , No. C 12-00790 SBA, 2012 WL 6019580 (N.D. Cal. Dec. 12, 2012)	25
<i>Parkstone v. Coons</i> , No. E2008-00894-COA-R3-CV, 2009 WL 1065941 (Tenn. Ct. App. Apr. 21, 2009)	15
<i>In re Pharmatrak, Inc.</i> , 329 F.3d 9 (1st Cir. 2003).....	13, 14, 15
<i>Phillips v. Cty. of Allegheny</i> , 515 F.3d 224 (3d Cir. 2008)	<i>passim</i>
<i>Pitt News v. Fisher</i> , 215 F.3d 354 (3d Cir. 2000)	8

<i>Ruiz v. Gap, Inc.</i> , No. 07-5739 SC, 2009 WL 250481 (N.D. Cal. Feb. 3, 2009)	30
<i>Scott v. Kuhlman</i> , 746 F.2d 1377 (9th Cir. 1984)	15
<i>Sheppard v. Google</i> , No. 4:12-CV-04022, 2012 WL 6086867 (W.D. Ark. Dec. 6, 2012)	32
<i>Shamrock Foods Co. v. Gast</i> , 535 F. Supp. 2d 962 (D. Ariz. 2008)	23
<i>Shefts v. Petrakis</i> , No. 10-CV-1104, 2013 WL 489610 (C.D. Ill. Feb. 8, 2013)	20
<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litig.</i> , MDL No. 11md2258 AJB (MDD), 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012)	30
<i>Stearns v. Ticketmaster Corp.</i> , 655 F.3d 1013 (9th Cir. 2011)	29
<i>In re Steroid Hormone Prod. Cases</i> , 181 Cal.App.4th 145 (2010)	34
<i>Stickrath v. Globalstar, Inc.</i> , 527 F. Supp. 2d 992	35
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004)	18
<i>Therapeutic Research Faculty v. NBTY, Inc.</i> , 488 F. Supp. 2d 991 (E.D. Cal. 2007)	17
<i>Thompson v. Home Depot, Inc.</i> , No. 07CV1058 IEG (WMc), 2007 WL 2746603 (Sept. 18, 2007)	30
<i>In re Toys R Us, Inc., Privacy Litig.</i> , No. 00-CV-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001)	25
<i>U.S. v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	17
<i>U.S. v. Students Challenging Reg. Agency Procedures(“SCRAP”)</i> , 412 U.S. 669 (1973)	8, 9

<i>U.S. v. Szymuskiewicz</i> , 622 F.3d 701 (7th Cir. 2010)	14
<i>U.S. v. Townsend</i> , 987 F.2d 927 (2nd Cir. 1993)	16
<i>Valentine v. NebuAd, Inc.</i> , 804 F. Supp. 2d 1022 (N.D. Cal. 2011)	32
<i>Wahl v. Am. Sec. Ins. Co.</i> , No. C 08-00555 RS, 2010 WL 1881126 (N.D. Cal. May 10, 2010)	28, 29
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	9, 10

STATUTES

18 U.S.C. § 1030(a) (1)-(7)	26
18 U.S.C. § 1030(a)(4)	25
18 U.S.C. § 1030(c)(4)(A)(i)(I-VI)	26
18 U.S.C. § 1030(e)(8)	24
18 U.S.C. § 1030(e)(11)	24
18 U.S.C. § 1030(g)	24, 26
18 U.S.C. § 2510(8)	16
18 U.S.C. § 2510(15)	20
18 U.S.C. § 2510(17)	19
18 U.S.C. § 2511 (1)(a)	14
18 U.S.C. § 2511 (1) (c)-(d)	14, 18
18 U.S.C. § 2511 (2)(d)	14
18 U.S.C. § 2701(a)	18, 19
18 U.S.C. § 2701(c)	23
Cal. Bus. & Prof. Code § 17200, <i>et. seq.</i>	28

Cal. Penal Code § 7.1	32
Cal. Penal Code § 502.....	11, 28, 30, 31
Cal. Penal Code § 502(a)	31
Cal. Penal Code § 502(b)(10)	31
Cal. Penal Code § 502(c)	31
Cal. Penal Code § 502(c)(1)	31
Cal. Penal Code § 502(c)(2)	31
Cal. Penal Code § 502(c)(6)	31
Cal. Penal Code § 502(c)(7)	31
Cal. Penal Code § 502(c)(8)	31
Cal. Penal Code § 502(e)(1)	31
Cal. Penal Code § 630.....	11, 28
Cal. Civ. Code § 1760.....	33, 34
Cal. Civ. Code § 1761(b)	34
Cal. Civ. Code § 1761(e)	34
Cal. Civ. Code § 1770.....	33, 35
Cal. Civ. Code § 1780(a)	33
Cal. Civ. Code § 1782.....	35
Cal. Civ. Code § 1782(d)	35

OTHER AUTHORITIES

132 Cong. Rec. H4039-01 (1986) 1986 WL 77650.....	13
<i>Black's Law Dictionary</i> 705 (4th ed. 1951)	21
Wright & Miller, <i>Federal Practice and Procedure</i> , § 1277	15

RULES

Fed. R. Civ. P. 8(a)(2).....	1, 3, 12, 19
Fed. R. Civ. P. 12(b)(1).....	1, 9
Fed. R. Civ. P. 12(b)(6).....	1, 3, 9

I. NATURE AND STAGE OF THE PROCEEDINGS

In this MDL, Plaintiffs timely filed their first Consolidated Amended Complaint (“CAC”) on December 19, 2012 (D.I. 46). Defendant Google filed a Motion to Dismiss pursuant to Fed. R. Civ. P. 12(b)(1),(6) (D.I. 57). Plaintiffs’ opposition is below.

II. SUMMARY OF ARGUMENT

1. Google’s Motion overstates Plaintiffs’ pleading burden under Rule 8(a)(2) and is based on contested factual issues and inferences requiring discovery that may not be resolved on a Rule 12(b)(6) motion.

2. Plaintiffs have pled injury-in-fact for Art. III standing and invasion of their own statutorily protected rights that alone suffices for statutory standing. The CAC shows specific values of the Personal Information Google impermissibly took, and specifically describes Google’s violation of Plaintiffs’ statutorily protected rights that provides standing.

III. CONTESTED AND UNSUPPORTED “FACTS” REQUIRE DISCOVERY

A. The Complaint’s Facts, Not Google’s, Control

Plaintiffs’ factual allegations are deemed true on this dismissal motion. *See Phillips v. Cty. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). Plaintiffs’ factual allegations differ fundamentally from Google’s factual arguments in virtually every respect, especially in Google’s misleading portrayal of its tracking cookies. Google secretly circumvented Apple’s Safari default blocker (CAC ¶¶ 68-126) and simultaneously deceived the IE browser (*id.* ¶¶ 171-190), using, respectively, hidden code that fooled the Safari browser into reacting as if the user was submitting an invisible “form” (*id.* ¶ 93) and “false P3P code” to deceive the IE browser into cookie acceptance (*id.* ¶¶ 183-187), about which users knew nothing, (*id.* ¶¶ 1, 3, 125) permitting Google’s tracking cookie placement. Google stopped only when caught and began removing the illicit cookies. *Id.* ¶ 119. Google implausibly defends its Safari hack by positing an

“unforeseen” and “unexpected” but massive and prolonged technological accident (D. Br. 6-7) by this self-described “global technology leader” (CAC ¶ 19), too sophisticated to “not anticipate this would happen” (*id.* ¶ 118), and which permitted Google to compete for its lifeblood advertising revenue (*id.* ¶¶ 14, 19, 117) against Facebook, which had already “come up with the now ubiquitous ‘Like’ button” (*id.* ¶¶ 100–04, 121). Google’s admits its IE hack, relying on an “everybody does it” defense (D. Br. 8; CAC ¶¶ 188-189) that depends on numerous facts the CAC contradicts (*see, e.g.,* CAC ¶ 187), unsupported assumptions (*see, e.g.,* D. Br. 8 (“Presumably, Microsoft does not strictly adhere to the P3P protocol...”), and Google’s factually unsupported “impracticality of compliance” assertion (CAC ¶ 189) about which Google never informed users. CAC ¶ 187 (Google’s P3P policy does not state Google’s intent).

Industry observers factually showed that Google’s Safari hack was intentional. *See* CAC ¶¶ 78, 105, 113, 116, 118, 120, 122-124. Google ad buyers knew nothing of Google’s trick and rejected it. *Id.* ¶¶ 125-126. Microsoft concluded Google intentionally tricked IE “employing similar methods” to those Google used against Safari. *Id.* ¶ 187. Revealing Google’s deceptive intent, Google said Safari users needed to do nothing to block unwanted cookies because Safari already blocked them, while at the same time Google was dismantling that block. *See, e.g., id.* ¶¶ 74–79, 83–89. The FTC’s \$22.5 Million fine against Google based on the same allegations (*id.* ¶¶ 163-170) confirms that the CAC’s facts, and their accompanying inferences, at a minimum “raise a reasonable expectation that discovery will reveal evidence” further supporting Plaintiffs’ claims. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 566 (2007).

Google’s detailed and fact-intensive brief demonstrates that Plaintiffs’ Complaint gives Google “‘fair notice’” of Plaintiffs’ claims and “‘the grounds on which [they] rest[].’” *Phillips v.*

Cty. of Allegheny, 515 F.3d 224, 231 (3d Cir. 2008) (quoting *Twombly*, 550 U.S. at 555).¹ Repeatedly emphasizing that notice pleading remains fundamentally intact (*Phillips*, 515 F. 3d at 230-234) and *Twombly*'s teaching that a complaint's facts need only be sufficiently "suggestive of the proscribed conduct" to raise the "reasonable expectation that discovery will reveal evidence" of the necessary elements (*id.* at 233-34), the *Phillips* court concluded: "Standards of pleading are not the same as standards of proof." *Id.* at 246.

B. Google's Cookies Permit User Tracking and Information Collection

Google's factual argument largely pivots on its mischaracterization of its cookies as inert internet nuts and bolts (D. Br. 3) that "collect" nothing: "The only thing Google obtained by virtue of the cookies' presence was the 'cookie value'—a string of characters that Google generates to identify an individual browser." D. Br. 1-2. *See also id.* 2 (cookies "have nothing whatsoever to do with content of any" Google-browser communications); *id.* 5 (DoubleClick ID cookie collects nothing); *id.* 9 (cookies neither "cause" nor "enable" Google's receipt of personal information); *id.* 10 (cookies only yield cookie values and alphanumeric chains). Google factually misrepresents its cookies' fundamental function of tracking users, gathering information and tying it to users. *See, e.g.,* CAC ¶¶ 38, 39(a)(ii), 39(b)(ii), 40, 45-48, 78, 96-99, 105, 109, 111-13, 124. Google solicits advertisers by bragging that Google can identify users for

¹ *Phillips* confirmed *Twombly*'s reaffirmation that Fed. R. Civ. P. 8(a)(2) requires only a "short and plain statement of the claim" that "does not require 'detailed factual allegations.'" *Id.* (quoting *Twombly*, 550 U.S. at 555). *Phillips* reiterated *Twombly*'s teaching that on this Rule 12(b)(6) motion, Plaintiffs' specifically-pleaded facts must be deemed true and their "complaint may not be dismissed merely because it appears unlikely that the plaintiff can prove those facts or will ultimately prevail on the merits." *Id.* (citing *Twombly*, 550 U.S. at 555, 563 n.8). *Phillips* confirmed that Plaintiffs receive the benefit of all "reasonable inferences." *Id.* *See also Golod v. Bank of Am. Corp.*, Civil No. 08-746 (NLH) (AMD), 2009 WL 1605309, at *1 (D. Del. June 4, 2009) (under "liberal federal pleading rules, it is not necessary to plead evidence," endorsing Rule 8(a)(2)'s "short and plain statement of claim" giving "fair notice" of claims and their grounds).

both Google and ad buyers using Google’s cookies. *Id.* ¶ 96. Google admits its cookies collect user information. *Id.* ¶ 98 n.67. Google admits it “may” combine user account information with “information from other Google services or third parties.” *Id.* CAC ¶ 98 n.67.

Google’s carefully parsed claim that “[t]he DoubleClick ID cookie itself neither contains nor collects any information” (D. Br. 5) trips not only on the CAC (¶¶ 1, 39, 45-48, 78, 96, 98, 98 n.67, 112, 113, 120-124) but on Google’s admission that its cookie *permits* collection of information. Google confirms cookies tie information to users: “cookie values” are transmitted “along with...Browser Generated Information” and Google’s DoubleClick ID Cookie lets Google “correlate the Browser-Generated Information for individual browsers.” D. Br. 4-5. Browser-Generated Information includes the address of the website the browser is displaying, which often reflects the nature, substance, or purport of the communication. *See* CAC ¶¶ 46-47, 98.

Google’s judicial notice materials more than “suggest” (*Phillips*, 515 F.3d at 233), they show, that Google’s cookies permit tracking. *See, e.g.*, Request for Judicial Notice (“RJN”) Ex. 2 at 2 (D.I. 58) (“Google Ads tracking cookie, *which monitors the browsing behavior of users going forward*” (emphasis added)); RJN Ex. 3 at 12 (Safari cookie blocking “would typically stop...doubleclick.net from tracking you”); RJN Ex. 4 at 4 (temporary cookie “could sometimes result in *extensive tracking of Safari users*” by opening door to “more cookies” (emphasis added)). Google’s server logs “may include” “one or more cookies that may uniquely identify your browser or your account.” RJN Ex. 1 at 2.

C. Google’s “Facts” are Unsupported or Contested

Google’s claims about its “new” “Intermediary Cookie” are unsupported. Google invented that innocent-sounding term, which appears nowhere in the CAC (or in any Google search results), to obscure the “Intermediary Cookie’s” status as just the sort of third-party

cookie Safari sought to block. Google admits its “Intermediary Cookie” linked “a user’s Google account (which may contain personal information) and the Google advertising network.” D. Br. 5. Google’s unsupported say-so that this supposedly “encrypted,” “temporary” cookie gathered no PII directly contradicts controlling CAC allegations. *See* CAC ¶¶ 84-94, 101-02, 113.

Google cites *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), written eleven years before Google’s browser circumventions, in claiming that “the DoubleClick ID cookie allows Google to recognize when browsers visit websites displaying ads from the Google advertising network and to correlate the Browser-Generated Information for individual browsers.” D. Br. 4. Ignoring the reason Google wanted this recognition – “to link Google’s general ad tracking cookie with the user’s account, producing personally-identifiable, user-specific information” (CAC ¶ 112 (quoting J. Mayer)) – Google does not say just what “correlate” means, a factual issue. Citing *In re DoubleClick* for the truth of facts about the DoubleClick ID cookie is impermissible. *See Leonard v. Stemtech Int’l, Inc.*, Civ. Action No. 12-86-LPS-CJB, 2012 WL 3655512, *3 n.6 (D. Del. Aug. 24, 2012) (court may take judicial notice of previous opinion on motion to dismiss only to establish opinion’s existence not for truth of opinion’s facts).

Google misleadingly cites CAC ¶¶ 84-94 and 101-02 in asserting that its supposedly beneficial “new” cookie “allowed [Google’s] distinct account and advertising systems to interact without commingling personal and anonymous data.” D. Br. 5. Those paragraphs say no such thing. Citing no support, and ignoring the Complaint’s abundant contrary facts (*see, e.g.*, CAC ¶¶ 105, 110-111, 113-126), Google says its “goal was to implement this personalization in a privacy and security sensitive manner.” D. Br. 5. Google’s claims that the “Intermediary Cookie collects no personal information, is not used to correlate Browser-Generated Information,

and is placed from the doubleclick.net domain” (D. Br. 5-6) are factually unsupported and contradict the CAC and Google’s own admission that its cookies collect information. CAC ¶¶ 98 n.67.

Google’s discourse on “The Safari Web Browser and How it Handles Cookies” (D. Br. 4-5) buries crucial facts (*e.g.*, Google’s deliberate use of a known Safari exception (CAC ¶¶ 92–93)), highlights uncontested ones (*e.g.*, Safari’s default setting), and relies on yet more supposed “facts” unsupported by any record, judicial notice, or common sense. *See* D. Br. 6–7 (“Unbeknownst to many, however, Apple had also relaxed Safari’s approach to third-party cookies by adopting another rule, unique among major browsers.”); *id.* 7 (“unforeseen consequence of Safari’s One In, All In Rule was that, once an Intermediary Cookie had been placed on a browser, certain Safari browsers would then accept the DoubleClick ID cookie,” an “unexpected outcome”). Google’s citation to CAC ¶¶ 179-84 contradicts Google’s assertion that Microsoft’s IE browser, in its default state, “usually allows third party cookies.” D. Br. 7.

Nothing in CAC ¶¶ 78, 105-06 supports Google’s proposition that web programmers knew about the Form Submission Rule and Facebook recommended the rule as a “best practice... for delivering a consistent user experience across all browsers.” D. Br. 6.

Google’s claim that Safari was “unique among major browsers” because it had “relaxed” its “approach to third-party cookies” through the “One In, All In Rule” in a manner that was “unbeknownst to many” is unsupported. D. Br. 7. Who, and how many, is “many”? Does “many” include Google personnel who developed the Safari hack?

Google offers only RJN Ex. 2, with no qualification, as the sole support for the supposition that, despite secretly using the Form Submission Rule to initiate the hack, “[t]he Google team that designed the Intermediary Cookie was unaware of Safari’s obscure and

atypical One In, All In Rule, and did not anticipate or intend that placing an Intermediary Cookie on a Safari browser could also cause the browser to accept a DoubleClick ID cookie.” D. Br. 7. RJN Ex. 2 does *not* say that Google’s team was unaware that its general Google Ads tracking cookie would follow the “Intermediate Cookie.” RJN Ex. 2 says only that “Google *stated* that they ‘didn’t anticipate that this . . . would happen.’” Google cites only CAC ¶ 105 in claiming that this result stemmed from “another quirk in Safari.” Read in full, CAC ¶ 105 and the article it quotes say no such thing.

CAC ¶¶ 179-84 do not say, as Google contends, that “[i]n its default state, Microsoft’s [IE] usually allows third party cookies.” D. Br. 7. They say the opposite: “[*b*]y default, IE is set to *block* third party cookies unless the site includes a P3P Compact Policy Statement.” CAC ¶ 180 (emphasis added). None of the other cited paragraphs say what Google claims. Google cites the CAC for the proposition that IE was “designed” to permit the deception that Google perpetrated to avoid IE’s cookie blocking. D. Br. 8. But those allegations, ¶¶ 183-84, show Google’s intentional use of false code (CAC ¶ 183) to “trick[] [IE] into believing Google’s doubleclick.net cookies are placed from a website which is P3P compliant.” CAC ¶ 184.

D. Plaintiffs Allege Personal and Direct Harm

Google wrongly claims Plaintiffs “do not allege that the DoubleClick ID Cookie or the Intermediary Cookie (or any other) was ever placed on their own browsers.” D. Br. 7. Describing cookie placements, the complaint specifically refers to “the case of Plaintiffs’ and Class Members” whom Google tracked “despite Plaintiffs’ and Class Members’ privacy settings in place to block this tracking scheme....” CAC ¶ 46. Google’s cookie placement on Plaintiffs’ browsers is encompassed by Plaintiffs’ factual allegations that they used Safari and Internet Explorer “to interact with the Internet” (*id.* ¶¶ 10–13), which, Google says, cookies facilitate. D. Br. 3. Google says cookies are “commonplace” and “regularly used.” D. Br. 3. Google confirms

it put cookies on Plaintiffs' browsers: "Assuming a browser's design and setting allow it to accept cookies, the DoubleClick ID Cookie will be placed on a browser during the normal exchange of information that accompanies the display of a Google ad in a browser." *Id.* 4.

IV. PLAINTIFFS HAVE PROPERLY ALLEGED STANDING

A. Plaintiffs Need Only Allege, Not Prove, "Identifiable Trifle" of Harm

Google's premature factual arguments that Plaintiffs "cannot show any injury" (D. Br. 12) and offer only "general allegations" of harm (D. Br. 12, 13) violate bedrock standing rules. First, at this initial stage, Plaintiffs need not prove but only *allege* an injury-in-fact. Plaintiffs have done so. *See, e.g.*, CAC ¶¶ 1-4; *Pitt News v. Fisher*, 215 F.3d 354, 360 (3d Cir. 2000), *cert. denied*, 531 U.S. 1113 (2001) (merits and standing are different inquiries; "[t]o demonstrate its standing to sue, a plaintiff must only *allege* that they have suffered sufficient injury to comply with Article III's 'case or controversy' requirement." (emphasis in original)); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) ("At the pleading stage, *general factual allegations* of injury resulting from Defendant's conduct may suffice, for on a motion to dismiss, 'we presume that *general allegations* embrace those specific facts that are necessary to support the claims.'" (quoting *Nat'l Wildlife Fed.*, 497 U.S. 871, 889 (1990)) (emphasis added)); *In re Ins. Brokerage Antitrust Litig.*, 579 F.3d 241, 275 (3d Cir. 2009) ("Plaintiffs only needed to allege that they suffered an injury in fact and were not required to prove the merits of their case . . . to establish standing.").

Second, Google's effort to raise standing's low bar ignores that Plaintiffs need only allege an "identifiable trifle" of harm. *See, e.g.*, *U.S. v. Students Challenging Reg. Agency Procedures* ("SCRAP"), 412 U.S. 669, 689 n.14 (1973)); *In re Global Ind. Tech., Inc.*, 645 F.3d 201, 210 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 551 (2011) ("injury-in-fact" is "some 'specific, 'identifiable trifle' of injury" (quoting *Bowman v. Wilson*, 672 F.2d 1145, 1151 (3d Cir. 1982)));

Bowman, 672 F.2d at 1151 (“contours of the injury in fact requirement . . . are very generous,” citing “identifiable trifle test); *Danvers Motor Co., Inc. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005) (“Injury-in-Fact is not Mount Everest.”). The fact, not amount, of injury provides standing. *See, e.g., U.S. v. SCRAP*, 412 U.S. at 689 n. 14 (rejecting limiting standing only to persons “significantly affected” by challenged action). If alleging losses of “a fraction of a vote,” “a \$5 fine and costs,” and “a \$1.50 poll tax” (*id.*) suffice for injury-in-fact, Plaintiffs’ allegations that Google secretly hacked into their personal computers and tracked and gathered their valuable personal information surely do. Google’s attempted shift of the injury inquiry to cookies alone and unwanted advertisements (D. Br. 2, 5, 7, 9) ignores the CAC.

Third, Google conflates Fed. R. Civ. P. 12(b)(1) jurisdictional standing analysis with the very different Fed. R. Civ. P. 12(b)(6) merits tests. *See, e.g., Warth v. Seldin*, 422 U.S. 490, 500 (1975) (“[S]tanding in no way depends on the merits of the plaintiff’s contention that particular conduct is illegal”); *Marion v. TDI, Inc.*, 591 F.3d 137, 149 (3d Cir. 2010), *cert. denied*, 131 S. Ct. 1479 (2011) (“merits” are “separate from the standing inquiry”). Google demands a hyper-factual specificity for Plaintiffs’ harm allegations (D. Br. 12, 13) that the law does not require. *See, e.g., Warth*, 422 U.S. at 501; *Maya v. Centex*, 658 F.3d 1060, 1067–68 (9th Cir. 2011) (*Twombly* and *Iqbal* are 12(b)(6) cases “ill-suited to application in the constitutional standing context”).

B. Plaintiffs Do Allege Personalized Harm

Citing *Warth*, Google claims Plaintiffs “fail . . . to allege facts showing they have ‘personally’ been harmed.” (D. Br. 12). Plaintiffs’ Complaint says otherwise. *See* CAC ¶¶ 2-4, 46. *Warth* is readily distinguished. *Warth*’s city taxpayer plaintiffs argued they had standing because they paid higher taxes because suburban exclusionary zoning resulted in disproportionately numerous low income people living in Rochester. Unlike *Warth*’s indirect

and attenuated harm, Plaintiffs here allege direct harm. *McNair v. Synopsis Grp., Inc.*, 672 F.3d 213 (3d Cir. 2012) (D. Br. 12) is an inopposite preliminary injunction case in which the plaintiffs alleged “wholly conjectural future injury.” *McNair*, 672 F.3d at 225.² Google invaded Plaintiffs’ computers and took their information. *See, e.g.*, CAC ¶¶ 1-5, 10-13, 68-126.

C. Plaintiffs Properly Allege Statutory Standing

Congress decided in the Wiretap and Stored Communications Acts that Defendants’ collection – through interception or improper access – of the contents of Plaintiffs’ communications is itself injury-in-fact in the form of invasion of protected statutory rights. Constitutional standing and statutory standing require distinct analyses. Google’s statutory standing argument impermissibly imposes a two-tiered injury requirement—alleged statutory violation plus “something else,” for example, *proven* statutory violation. D. Br. 12 n.8. *Warth* and its many progeny reject such a rule. *See Warth*, 422 U.S. at 500 (“Congress may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the Plaintiff would have suffered no judicially cognizable injury in the absence of [the] statute.”). *See also, Lujan*, 504 U.S. at 578. Google ignores *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 763 (3d Cir. 2009), holding that allegations the defendant invaded plaintiffs’ statutorily protected right to a real estate settlement “free of unlawful kickbacks and unearned fees,” without actual financial loss or other injury, sufficed for statutory standing. *See also*

² Unlike Plaintiffs’ case of direct and completed injury, *Clapper v. Amnesty Int’l. USA*, 133 S. Ct. 1138 (Feb. 26, 2013), illustrates indirect and future harm insufficient for standing. Lawyers, human rights workers and others claimed that government surveillance of their out-of-country clients might lead to interception of their communications, but only if the government did imminently target these clients, used the challenged surveillance method, the FISC authorized the surveillance, the surveillance succeeded, and captured Plaintiffs’ communications.

Edwards v. First Am. Corp., 610 F.3d 514, 516–17 (9th Cir. 2010); *Gaos v. Google*, No. 5:10-CV-4809, 2012 WL 1094646, *3 (N.D. Cal. Mar. 29, 2012).

Plaintiffs’ have pleaded statutory standing through an invasion of their own statutory rights under the Wiretap Act (Count I, CAC ¶¶ 198-212), Stored Communications Act (Count II, CAC ¶¶ 213-219), Computer Fraud and Abuse Act (Count III, CAC ¶¶ 220-227), California Unfair Competition Law (Count VI, CAC ¶¶ 238-250), California Penal Code §502 (Count VII, CAC ¶¶ 251-264); California Penal Code § 630 (Count VIII, CAC ¶¶ 265-274); and California Civil Code §1750 (Count IX, CAC ¶¶ 275-283). These allegations suffice for injury in fact. Nothing more is required. *See, e.g., Alston*, 585 F.3d at 763.

Google’s argument that PII is valueless so its deprivation imposes no harm (D. Br. 13-15) cannot trump Plaintiffs’ factual allegations showing otherwise (CAC ¶¶ 49-67), Google’s own payments for PII (CAC ¶¶ 57-60), and contrary case law. *See, e.g., Claridge v. RockYou*, 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011) (breach of PII sufficed for Art. III standing). Recent industry studies not available before show that PII has identifiable value to Plaintiffs (CAC ¶¶ 56-67), which was not present in the cases Google cites.

Google invites the Court to focus on cookies in isolation from the personal information those secret cookies permitted Google to collect. D. Br. 9, 12. Google’s claim that “the CAC show[s] that Google obtained no personal information by placing the cookies on browsers” wishes away Plaintiffs’ factual allegations of this data collection (CAC ¶¶ 78, 86-98), which industry experts confirmed. *See* CAC ¶ 113 (secret cookies produced collection of “identifying and identifiable information.”); *id.* ¶ 122 (Google “was quite intentionally moving information about a Google user’s account over to Google’s advertising networks”); *id.* ¶ 123(a) (“Google is leveraging user account information to personalize its advertising on non-Google websites.”); *id.*

¶ 123(b) (Google “intentionally bypassed” Safari cookie blocker “to place an identifying cookie that it uses for social advertising”).

Google cites *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5-6 (N.D. Cal. Dec. 28, 2012), as holding that “Article III’s standing requirement is not satisfied unless a Plaintiff’s allegations establish that the statute has actually been violated.” D. Br. 12 n.8. Neither *Google* nor any case can permissibly import factual merits analysis—whether a law “has actually been violated”—into Art. III standing analysis at the pleadings stage. Comporting with Rule 8(a)(2), numerous cases teach that Plaintiffs’ burden is minimal at the pleadings stage and increases through summary judgment and trial. *See, e.g., Lujan*, 504 U.S. at 578 (differentiating “the manner and degree of evidence required at the successive stages of the litigation,” emphasizing “general factual allegations of injury suffice at pleading stage,” distinguishing pleadings stage from summary judgment). *See also Bennett v. Spear*, 520 U.S. 154, 168 (1997) (general allegations of diminution in water sufficed for standing because “easy to presume specific facts under which plaintiffs will be injured”).

D. Google’s Cited Cases Do Not Support Google’s Standing Argument

Plaintiffs’ factual allegations about PII’s market and dollar values (CAC ¶¶ 49-67) are far more specific than those at issue in Google’s cited cases. Unlike Plaintiffs here, the plaintiffs in *LaCourt v. Specific Media, Inc.*, No. SACV10-1256, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), did not allege they were personally affected by defendants’ practices violating specific statutes, making only “tepid” and “half-hearted” harm allegations. They “more or less completely accepted Defendants’ framing of the issue.” *LaCourt*, 2011 WL 1661532 at *4. Even so, the *LaCourt* panel said it “probably would decline to say that it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant’s alleged practices, but “at this point they have not done so.” *Id. Del Vecchio v. Amazon.com Inc.*,

No. 11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (“*Del Vecchio I*”), did not involve specific allegations of admitted cybersnooping that just happened to permit Google to compete with its main rival, and was punished with a \$22M fine by the FTC (CAC ¶¶ 163-170), the harm from which Google admitted by agreeing to remove the illegally planted cookies. CAC ¶ 119. Unlike *Del Vecchio I*’s plaintiffs, Plaintiffs here plead facts generating the reasonable inference that Plaintiffs’ PII lost value as a result of Google’s collection of data. CAC ¶¶ 49-67. Google itself pays users for PII. CAC ¶¶ 57-60.

V. LEGAL ARGUMENTS

A. **Count I – The Complaint States A Claim Under The Electronic Communications Privacy Act (“ECPA”), 18. U.S.C. § 2510 Et Seq.**

“The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.” *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). Enacted in 1986, the “ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications.” *Id.*³

The CAC’s facts show: (1) Google intercepted the “contents” of communications between Plaintiffs and first-party websites by transmitting hidden code that tricked Plaintiffs’ browsers’ “do not track settings” (*see, e.g.*, CAC ¶¶ 199-202); (2) Google was not a party to the communications it intercepted or Google would not have needed to trick Plaintiffs’ browsers; and, (3) neither Plaintiffs (*Id.* ¶ 204) nor the websites (*Id.* ¶¶ 126, 210) knew of or consented to

³ “[L]egislation which protects electronic communications from interceptions...should be comprehensive, and *not limited to particular types or techniques of communicating*....Any attempt to...protect only those technologies which exist in the marketplace today...is destined to be outmoded within a few years....what is being protected is *the sanctity and privacy of the communication*. We *should not attempt to discriminate for or against certain methods of communication*....” 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Representative Kastenmeier) (emphasis added).

Google's clandestine interceptions. Having pleaded facts showing an unlawful interception, Plaintiffs may also plead use and disclosure claims under 18 U.S.C. § 2511 (1) (c)-(d).⁴

1. Google Was Not a Party to the Communication; It May Not Manufacture a Statutory Exception Through Its Own Illegal Conduct

Google invokes a Wiretap Act exception (18 U.S.C. § 2511 (2)(d)) protecting a communication's intended recipient. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). But the CAC shows that Google was not an intended party to Plaintiffs' communications with first-party websites and that Plaintiffs' browsers were specifically configured to *prohibit* Google from becoming a party to them. CAC ¶¶ 69-73, 180, 199. Google only gained access to Plaintiffs' communications by designing code that tricked Plaintiffs' web browsers into sending Plaintiffs' communications with first-party websites to Google. CAC ¶¶ 84-99, 183-188, 201-203. Google cannot manufacture a statutory exception to the Wiretap Act through its own misconduct. *See In re iPhone Application Litig.*, 844 F.Supp.2d at 1062 (where plaintiffs had not intended any communication, a Wiretap Act defendant like Apple "cannot manufacture a statutory exception through its own accused conduct").⁵

⁴ Google does not claim that Plaintiffs have not properly pled the "device" element. *See U.S. v. Szymuskiewicz*, 622 F.3d 701, 707 (7th Cir. 2010). Nor does Google say no "interception" occurred. *See id.* at 705-06; *see also In re Pharmatruk*, 329 F.3d at 21-22; *In re Doubleclick*, 154 F. Supp. 2d at 514 (DoubleClick conceded its conduct violated 18 U.S.C. § 2511 (1)(a)).

⁵ *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011), is inapposite. The plaintiff there alleged a Wiretap Act violation against a defendant with whom plaintiff intended to directly communicate. *Id.* at 713. Here, the facts show interception despite Plaintiffs' browsers efforts to exclude Google from the communication. Google offers the remarkable proposition that a browser's GET request for an ad makes Google a party to subsequent communications that browsers were specifically attempting to block. A medical patient may consent to one form of treatment and refuse another. So too may a web user consent to one form of communication but not another. *See In re Pharmatruk*, 329 F.3d at 19.

2. Google Did Not Have Prior Consent from a Party to the Communication

Google bears the burden of establishing the affirmative defense of the separately stated consent exception in 18 U.S.C. § 2511(2)(d). *See Pharmatrak*, 329 F.3d at 19. That exception is not appropriately the subject of this motion.⁶ *See, e.g., Scott v. Kuhlman*, 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, *Federal Practice and Procedure*, § 1277 at 328-30) (affirmative defenses may not be raised in a motion to dismiss unless there are no disputed issues of fact). Google’s argument boils down to the remarkable proposition that the CAC does not disprove Google’s fact-intensive affirmative defense.

Nevertheless, consent “should not be casually inferred.” *In re Pharmatrak*, 329 F.3d at 20. Emphasizing the factual nature of consent, courts employ a two-part inquiry: (1) establish the “dimensions of consent”; and (2) “ascertain whether the interception exceeded those boundaries.” *Id.* at 19. Google – which never claimed “consent” when its hacking was discovered (CAC ¶¶ 115, 119) – erroneously infers unlimited consent for tracking Plaintiffs’ substantive communications with websites from Google’s receipt of a GET request for an ad. However, Plaintiffs’ settings vitiated user consent to Google tricking Plaintiffs’ browsers into accepting tracking technology the browser was configured to block. Websites “were not aware of this behavior,” “would never condone it,” and “told Google [they] don’t support this

⁶ Even when a defendant can prove consent, the plaintiff may overcome it by proving the exception to the exception—that the interception was done for the “purpose of committing a criminal or tortious act.” 18 U.S.C. § 2511 (2)(d). Google’s invasion of Plaintiffs’ privacy for commercial gain is such a tortious act. *See, e.g., Parkstone v. Coons*, No. E2008-00894-COA-R3-CV, 2009 WL 1065941, *6 (Tenn Ct. App. Apr. 21, 2009) (four variants of privacy torts under Delaware law); *Bagramian v. Legal Recovery Law Offices, Inc.*, No. CV 12-1512-CAS (MRWx), 2013 WL 550490, at *5 (C.D. Cal. Feb. 11, 2013) (two invasions of privacy torts under California law).

activity.” CAC ¶ 126. Google has provided no evidence that *any* website consented to its conduct, let alone *all* of them consented. Plaintiffs are entitled to discovery on this factual issue.

Finally, Google’s reliance on *In re DoubleClick* is misplaced. *See* 154 F. Supp. 2d at 504-05. Decided more than ten years ago, before Google’s development of its surreptitious technology to evade cookie blocking, that case did not involve the intentional circumvention of privacy settings. To the contrary, the court emphasized:

DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick’s tracking. As plaintiffs’ counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways:...(2) ***configuring their browsers to block any cookies from being deposited.***

Id. (emphasis added). Here, the CAC alleges Google/DoubleClick were doing exactly that (collecting information from users who took “simple steps to prevent DoubleClick’s tracking” by “configuring their browsers to block any cookies from being deposited”) which the *DoubleClick* court was led to believe was not occurring there.

3. Google Intercepted⁷ the “Content” of Communications

The Wiretap Act defines “contents” to mean “information concerning the substance, purport, or meaning of” a communication. 18 U.S.C. §2510(8). Google factually and mistakenly contends it intercepted “mere transactional information,” then invokes inapplicable precedent saying such information is not “content.” Google did intercept transactional information. However, Google *also* intercepted “contents.” *See, e.g.*, CAC ¶¶ 45-48, 78, 98, 98

⁷ Google relegates to a footnote its argument that Plaintiffs have not pled an “intentional” interception. For an intentional interception, the defendant must have acted deliberately and purposefully, its act the product of conscious objective rather than mistake or accident. *See U.S. v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993). The CAC contains many facts showing Google deliberately, purposefully and consciously tricked Plaintiffs’ web browsers in order to intercept Plaintiffs’ communications with other websites. *See, e.g.*, CAC ¶¶ 113 -124. At a minimum, Plaintiffs are entitled to discovery on intent.

n.67, 123-124.

Google’s circumvention of Plaintiffs’ browsers’ settings allowed it to intercept: (1) the specific URLs that Plaintiffs requested from websites, which identified “specific items, such as websites, videos, pictures, or articles”; and (2) “information that Class Members exchanged with first-party websites during the course of filling out forms or conducting searches.” CAC ¶¶ 205–07. Defendant intercepted “not just the fact of a request, but the exact request itself, which, because it includes descriptive URL information, is substantive.” *Id.* ¶¶ 47, 207.

Courts have recognized that URLs constitute “content.” *U.S. v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008), *cert. denied sub nom*, 129 S. Ct. 249 (2008) (URL constitutes “content” because URL “identifies a particular document within a website that person views and reveals much more information about a person’s Internet activity”); *In re Application of the United States for an Order Authorizing the Use of a Pen Register and Trap*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (URL constitutes “content” because the “substance” and “meaning” of the communication is that the user is conducting a search for information on a particular topic). Plaintiffs have pleaded how the interception of URLs equates to an interception of content. CAC ¶¶ 47, 98, 207. A URL reveals the “content,” the “substance, purport, [and] meaning” of the communication.⁸

Finally, Defendant factually and inaccurately claims that the only additional information it gained from its surreptitious code was the value of the resulting secretly implanted cookies. The CAC shows Google intercepted URL strings and information contained in online forms. In

⁸ In *Brown v. Waddell*, 50 F.3d 285, 287-88 (4th Cir. 1995), police obtained “pager clones” that intercepted additional number codes, one of which indicated that a caller was “en route.” The court found these additional numbers were “contents” under the Wiretap Act. *Id.* at 294. If numbers on a pager are “content,” so are the words and numbers in a URL string.

bypassing browser privacy settings, Google was then able to place other cookies, including its “id” cookie, a “unique and consistent identifier given to each user by Google for its use in tracking persons across the entire spectrum of websites on which Google places doubleclick.net cookies.” CAC ¶ 94. Providing Google with much more than a string of numbers, this cookie value is a virtual Rosetta Stone, allowing Google to associate vast amounts of communications content (e.g., URL strings it has collected) with specific, identifiable users (CAC ¶¶ 98, 98 n. 67, 205, 209) who had no reason to suspect that Google was secretly tracking their online activities.

4. The Complaint’s Facts Showing Improper Interception Authorize Use and Disclosure Allegations.

Google premises its use and disclosure argument (D. Br. 19) on its factually unsupported assertion that it was party to, or had consent to track, Plaintiffs’ communications. Because Plaintiffs pleaded facts that must be taken as true and establish unlawful interceptions, Plaintiffs may also assert use and disclosure allegations under 18 U.S.C. § 2511 (1)(c)-(d). *See Bartnicki v. Vopper*, 532 U.S. 514, 520, 525 (2001). Google inappositely cites cases in which a known party to a telephone conversation recorded it. Plaintiffs did not know Google had made itself a party to Plaintiffs’ communications.

B. COUNT II - PLAINTIFFS HAVE PLED A CAUSE OF ACTION UNDER THE STORED COMMUNICATIONS ACT (“SCA”)

“[T]he Stored Communications Act protects individuals’ privacy and proprietary interests.” *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). It provides a cause of action against “whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. . . .” 18 U.S.C. §

2701(a). The statute “was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.” *Crispin v. Christian Audiger, Inc.*, 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010) (citations omitted). The “sort of trespasses to which the [ECPA] applies are those in which the trespasser gains access to information . . . which he is not entitled to see.” *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 997 (E.D. Cal. 2007).

1. Google Accessed Information in “Electronic Storage”

“Electronic storage” includes “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof...” 18 U.S.C. § 2510(17). Plaintiffs pleaded what the SCA requires: facts showing that the data Google accessed without authorization was temporarily stored pending delivery. CAC ¶ 218. Plaintiffs allege extensive factual details explaining how Google gained unauthorized access (CAC ¶¶ 27-48, 68-126, 171-190) and how the information accessed was stored. CAC ¶¶ 45-46, 94-97, 176, 187-188. Plaintiffs have met their burden of *pleading* that Google impermissibly accessed Plaintiffs’ information in temporary “electronic storage.” *See, e.g., Phillips*, 515 F. 3d at 230. *See also Golod*, 2009 WL 1605309, *1; *Expert Janitorial LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740, *3, *5 (E.D. Tenn. Mar. 12, 2010) (“for purposes of a motion to dismiss, plaintiff’s allegations [under the SCA] that the email accounts, user-names, and passwords were stored on plaintiff’s computers and that defendants knowingly accessed this stored information without authorization are sufficient allegations to assert a claim under § 2701”).⁹ *See also In re Intuit*

⁹ *In re DoubleClick* is not to the contrary. (D. Br. 20-21.) *DoubleClick’s* plaintiff alleged that the data files (cookies) at issue were *permanently* stored on their hard drives, leading the court to conclude, as a matter of law, that the defendants could not have accessed information in temporary “electronic storage.” *In re DoubleClick*, 154 F. Supp. 2d at 512. Here, Plaintiffs specifically allege that the cookies were temporarily stored on their computing devices when

Privacy Litig., 138 F.Supp.2d 1272, 1277 (C.D. Cal. 2001) (“Plaintiffs have alleged that Defendant accessed data contained in ‘cookies’ that it placed in Plaintiffs’ computers’ electronic storage. The court concludes that this allegation satisfies the liberal requirements of Rule 8(a)(2).”)

The cases Google cites are inapposite. *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 2012), and *Freedom Banc Mortg. Servs., Inc. v. O’Harra*, No. 2:11-CV-01073, 2012 WL 3862209 (S.D. Ohio Sept. 5, 2012), both state that if the accessed files are stored *by the electronic communication service provider*, in this case Google¹⁰, for its future use, as Google stores cookies in the browser-managed files, the definition of a “facility through which an electronic communication service is provided” applies. *Garcia*, 702 F.3d at 793; *O’Harra*, 2012 WL 3862209 at *8-9. Only Google can store the cookies at issue. Plaintiffs were not even aware of their unauthorized placement. The browser-managed files storing the cookies, which are the “facilities” Plaintiffs alleged were accessed without authorization (CAC ¶ 217), are within the SCA’s “electronic storage.” *Compare Shefts v. Petrakis*, No. 10-CV-1104, 2013 WL 489610, at *3 (C.D. Ill. Feb. 8, 2013) (summarizing *Garcia*, 702 F.3d at 793: “In addition, because the communications on the plaintiff’s phone were not being stored there *by her* electronic communication service provider, they were not in protected “electronic storage” and were thus outside the scope of the SCA.” (emphasis in original)).

2. Browser-Managed Files on Computer and Mobile Devices are “Facilities” Under the SCA

Google accessed them without permission. CAC ¶ 167.

¹⁰ Google is an “electronic service provider” under the SCA. An electronic communications service (“ECS”) is “any service which provides to users thereof the ability to send or receive wire or electronic communications[.]” 18 U.S.C. § 2510(15). *See, e.g., Garcia*, 702 F.3d at 792 (“Courts have interpreted the statute to apply to providers of a communication service such as . . . Internet or e-mail service providers.”).

Google argues Plaintiffs fail to allege Google accessed a “facility.” Google ignores Plaintiffs’ allegation that Google’s “browser-managed files” are the “facilities” under the SCA, not the computing devices themselves. *See* CAC ¶ 217. When Google tricks a browser into allowing its unauthorized third-party tracking cookie, Google stores information about the user’s activity in these browser-managed files. Google possesses user information through its browser-managed files. Google accesses “a facility through which an electronic communication service is provided,” *i.e.*, Plaintiffs’ browser-managed files on their computing devices.

The SCA does not define “facility.” Black’s Law Dictionary defines “facilities” as that “which promotes the ease of any action, operations, transaction or course of conduct. The term denotes inanimate means rather than human agencies.” *Black’s Law Dictionary* 705 (4th ed. 1951). “Congress intended the term to include the physical equipment used to facilitate electronic communications.” *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334 (D.D.C. 2011). Here, Plaintiffs allege a detailed communication system including many items of “physical equipment,” including the user’s hardware, and within it the browser-managed files, resulting in Google’s accessing information the SCA prohibits. Google without authorization stores a cookie in a user’s browser-managed files and obtains information through those cookies. CAC ¶¶ 27-48, 68-126, 171-90. Google’s own description of cookies shows they are “equipment used to facilitate electronic communications.” D. Br. 3-4 (“cookie value” with “Browser-Generated Information” is “useful” because permits correlat[ion] of information with individual browser and delivery of tailored content).

Avoiding Plaintiffs’ actual allegations regarding “browser-managed files,” (*see* CAC ¶¶ 217-18), Google asserts that a computer or mobile device is not a “facility through which an electronic communication service is provided.” D. Br. 21. Plaintiffs’ browsers, and Google’s

cookies/browser-managed files, are facilities through which Google provides an electronic communication service and tailored ads. Computers and mobile phones on which Google's browser-managed files are stored are SCA "facilities," so those files themselves must be also. *See Cousineau v. Microsoft Corp.*, No. C11-1438-JCC, at 10-11 (W.D. Wash. June 22, 2012) (See Ex. A attached hereto) ("Congress chose a broad term—facility—where it intended the statute to cover a particular function, such as internet access, as opposed to a particular piece of equipment providing that access, such as a router, laptop or smart phone. As technology evolves, identifying a smart phone as a facility through which an ECS is provided is not as 'strained' as it once may have seemed.").¹¹ Finding that a computer was a "facility," the *Cousineau* court said: "While earlier stages of technological development may have required large facilities for data storage, the draw of mobile devices is that their smaller storage space enables communication and information access regardless of the user's location." *Id.* at 11.¹² Plaintiffs allege the SCA paradigm: Google, the provider; Plaintiffs, the users; and Google's possession, through its browser-managed files, of the Plaintiffs' information. *Garcia*, 702 F. 3d at 793 (citing Kerr, *A User's Guide to the [SCA]*, 72 Geo. Wash. L. Rev. 1208, 1215 (2004).

¹¹ *See also Chance v. Avenue A, Inc.* 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (SCA's definition of "facilities" includes personal computers); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001) ("The court notes, however, that Section 2701 does not require that Plaintiffs' computers be 'communication service providers' only that they be a **facility** through which an electronic communication service is provided.") (emphasis in original); *Expert Janitorial, LLC*, 2010 WL 908740, *5 (citing *In re Intuit* and holding "plaintiff's computers on which the data was stored may constitute 'facilities' under the SCA").

¹² *Garcia* and *O'Harra* are distinguishable. Plaintiffs' allegations relate to files Google stores in Plaintiffs' browser-managed files. *Garcia* is factually different. Google secretly places the browser-managed files/cookies, then secretly accesses them to possess user information. *Garcia* put her own materials on her own phone, meaning the hack had to come from farther "outside." Moreover, *Garcia* is a summary judgment, not a motion to dismiss, ruling. *Garcia*, 702 F.3d at 790. The storage in *O'Harra* was by plaintiff on plaintiff's own hard drives, different from Google's storage of user information on Google's own illicitly implanted browser-managed files, which are facilities providing communications service and targeted ads.

Discovery will further show that these physical means of communication constitute a “facility.” *Gaubatz*, 793 F. Supp. 2d at 336 (denying motion to dismiss because defendants’ argument that plaintiffs’ own office computers are not a “facility” “may or may not turn out to have merit upon further development of the factual record”); *see also Cousineau*, NO. C11-1438-JCC, slip op. at 12.

3. Google’s Access Was Not Authorized

Google’s assertion that it was authorized to access its own cookies ignores their illicit placement. Google again relies on *In re DoubleClick*, 154 F. Supp. 2d 497. But Google’s surreptitious bypassing of the browser configurations *DoubleClick* suggested could block the collection of information (*id.* at 504-05) defeats Google’s *ipse dixit* (we did it, so it was authorized) authorization claim. Plaintiffs allege, and Google can show, no “conduct authorized” under 18 U.S.C. § 2701(c). Google is not the “intended” recipient of communications that Google assured users (CAC ¶ 79) Plaintiffs’ browsers would block. *See* CAC ¶¶ 69-73.

C. COUNT III - PLAINTIFFS HAVE STATED A CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT (“CFAA”)

Google initially contends that the CFAA is limited to “hacking,” arguing that the statute “was enacted to address classic computer hacking” and that the CFAA remains primarily a criminal statute designed to combat hacking. D. Br. 22. Any common sense interpretation of “hacking” includes Google’s “secret code-disabling-Safari privacy-followed-by-secret-tracking cookie” scheme. CAC ¶ 111. Google offers no definition of “hacking,” save one case citation that noted legislative history equated “hacking” to “breaking and entering.” D. Br. 22 (citing *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965-66 (D. Ariz. 2008)). Google omits *Shamrock’s* damaging full citation: “[t]he general purpose of the CFAA was to create a cause of

action against computer hackers (e.g. electronic trespassers)” and that “the conduct prohibited is analogous to that of breaking and entering rather than using a computer.” *Shamrock*, 535 F. Supp. 2d at 965 (internal citations omitted). *Shamrock* teaches that “hacking” includes Google’s “electronic trespassing,” which is cyberspace’s equivalent to “breaking and entering,” far beyond mere use of a computer. *See* CAC ¶¶ 74-78, 83-126. Sufficing for their CFAA claim, Plaintiffs allege, with strong industry observer support (CAC ¶¶ 105, 113, 116, 120, 122, 123,124), that Google intentionally wrote its code to trick Safari and IE. *Id.* ¶ 77, 187.

1. Plaintiffs Have Alleged Sufficient Damage or Loss

The CFAA provides a civil remedy for “[a]ny person who suffers damage or loss by reason of a violation of this section[.]” 18 U.S.C. § 1030(g). “Damage” is “any impairment to the integrity or availability of data, a program, a system, or information[.]” 18 U.S.C. § 1030(e)(8). “Loss,” separately, is “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any other revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]” 18 U.S.C. § 1030(e)(11).

Plaintiffs allege and Google’s history (CAC ¶¶ 163-170) demonstrates that “Google’s privacy violations here are part of a systemic business model that depends centrally on gathering reams of private data that informed users would not knowingly give up, at least without payment.” CAC ¶ 163. Google’s impairing the integrity of Plaintiffs’ browser “system” through illicit cookies and of Plaintiffs’ “data” or “information” through unpermitted capture and use underscores Plaintiffs’ statutory “damage.”

The CFAA imposes a civil penalty for anyone who “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and

by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period[.]” 18 U.S.C. § 1030(a)(4). Google contends Plaintiffs have failed to allege a \$5,000 economic loss. D. Br. 23-24. Plaintiffs allege Google knowingly and intentionally accessed protected computers, without or in excess of authorization, and obtained valuable information through unpermitted third-party cookies. CAC ¶¶ 49-67. “[B]ecause [plaintiff] alleges that [defendant] obtained something of value beyond solely the use of the computer, the \$5,000 requirement . . . is inapposite. Accordingly, the Court rejects [defendant]’s contention that [plaintiff]’s CFAA claim is subject to dismissal for failure to properly allege damages.” *Oracle Am., Inc., v. Service Key, LLC*, No. C 12-00790 SBA, 2012 WL 6019580, at *4 (N.D. Cal. Dec. 3, 2012).

Anyway, Plaintiffs do allege the data Google obtained is worth far more than \$5,000. CAC ¶¶ 49-67. Plaintiffs specifically allege that the “monetary and trade value of the information that Defendants take from users is well understood in the e-commerce industry” (*id.* ¶ 49) and that the cash value of this personal information has recently been quantified as high as \$4.20 per year for contact information, \$3.00 per year for demographic information and \$52.00 per year for web browsing histories. *Id.* ¶ 56. Google relies on *In re DoubleClick* and its progeny to argue that Plaintiffs cannot aggregate losses across the putative class. D. Br. 24 n.12. The *In re DoubleClick* court concluded that the CFAA “only allows aggregation of damage over victims and time for a single act.” 154 F. Supp. 2d at 524. Google’s intentional circumvention of Safari and IE are each a “single act” permitting aggregation of damages. *See, e.g., In re Apple & AT&TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (legislative history confirms Congress intended damages aggregation); *In re Toys R Us, Inc., Privacy Litig.*, No. 00-

CV-2746, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001).

2. Plaintiffs Allege Sufficient Facts To Support Their CFAA Claim

“[T]he CFAA... creates a private right of action for persons injured by conduct prohibited thereunder.” *Oracle Am.* at *3 (citing 18 U.S.C. § 1030(g)). A CFAA plaintiff must allege that defendant violated one of the provisions of § 1030(a)(1)-(7) and involving one of the factors in § 1030(c)(4)(A)(i)(I-VI). *Id.* (citations omitted).

a. Plaintiffs Have Alleged Both Transmission Offense and Unauthorized Access Offense

Plaintiffs allege that “Defendants intentionally accessed Plaintiffs’ and Class Members’ computers without authorization or exceeded authorized access to such computers” and that Defendants “knowingly caused the transmission of a program, information, code or command.” CAC ¶¶ 224-226.

Google again contends that Plaintiffs fail to “show” intentional damage-causing conduct. D. Br. 25, 26. First, Plaintiffs are not required to “show” but need only allege enough facts to suggest a plausible claim of intent. Plaintiffs have alleged Google’s specific intentional misconduct. CAC ¶¶ 3, 100-125. Plaintiffs allege “a scheme by which Defendants were bypassing the privacy settings of tens of millions of people who use Apple’s Safari web browser to use the Internet” and that Defendants “exploited” an exception to Apple’s privacy technology by “adding code to ads that tricked Safari into believing the exception had been satisfied.” CAC ¶¶ 76-77. Plaintiffs delineate Google’s systematic process to circumvent the Apple privacy settings by which, upon receipt of a “GET request,” Google inserted code into the webpages. *Id.* ¶¶ 83-87. *See also* ¶¶ 183-189 (same as to IE and Google’s P3P scheme). Far more than mere “labels and conclusions” (*Twombly*, 550 U.S. at 555), these allegations properly allege Google’s intentional conduct.

Google's argument that "Plaintiffs cannot show that Google accessed their computers 'without authorization'" or exceeded such authorization (D. Br. 25-26) also fails. Google specifically said that Safari users' privacy settings would be secure (CAC ¶ 79), and then affirmatively circumvented those settings. The FTC charged that "despite these promises . . . Google placed advertising tracking cookies on consumers' computers, in many cases by circumventing the Safari browser's default cookie-blocking setting." CAC ¶ 167.

D. COUNTS IV & V - PLAINTIFFS HAVE PROPERLY PLED CAUSES OF ACTION FOR INVASION OF PRIVACY & INTRUSION ON SECLUSION

On November 7, 1972, article I, section I, voters amended the California Constitution to include privacy as an inalienable right (the Privacy Initiative). *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 15, 21 (1994), shows the impetus was conduct just like Google's:

"The principal focus of the Privacy Initiative is readily discernible . . . unnecessary information gathering . . . computer stored and generated dossiers and cradle-to-grave profiles on every American dominate the framers' appeal to the voters. The evil addressed is . . . business conduct in collecting and stockpiling unnecessary information The Privacy Initiative's primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."

"Legally recognized privacy interests [include] conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Id.* at 35.

"[A] plaintiff alleging an invasion of privacy in violation of the state constitutional right to privacy must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Id.* at 39-40. Plaintiffs' Complaint satisfies all three elements. First, Plaintiffs have a legally protected right to be free of Google's "information gathering" and to conduct personal activity (web browsing) "without observation" by Google. *Id.* at 21. Second, Plaintiffs have a reasonable expectation of privacy; their browsers' default

settings prohibited Google's tracking cookies (CAC ¶¶ 68-73) and Google hid its tracking. CAC ¶¶ 1, 74-78, 83-126. Finally, Google's privacy invasion was serious because freedom from unnecessary information gathering is the core value furthered by the Privacy Initiative.¹³

E. COUNT VI - PLAINTIFFS HAVE PROPERLY PLED A CALIFORNIA UNFAIR COMPETITION LAW CLAIM ("UCL")

Plaintiffs adequately plead a claim for breach of California's Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et. seq.*) ("UCL"). Under the UCL, any person or entity that has engaged, is engaging, or threatens to engage "in unfair competition may be enjoined in any court of competent jurisdiction." *Id.* §§ 17201, 17203. "Unfair competition" includes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." *Id.* § 17200. The UCL's "broad scope . . . allows for violations of other laws to be treated as unfair competition . . . while also sweep[ing] within its scope acts and practices not specifically proscribed by any other law." *Hauk v. JPMorgan Chase Bank USA*, 552 F.3d 1114, 1122 (9th Cir. 2009) (quoting *Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 949 (2002)).

Any illegal business practice *per se* violates the UCL. *Kasky*, 27 Cal. 4th at 950. Plaintiffs allege that Defendants violated the unlawful prong of the UCL by violating the California Consumers Legal Remedies Act, Cal. Penal Code § 502 and 630, *et seq.*, 18 U.S.C. 2510, *et seq.*, and 18 U.S.C. 1030, *et seq.* See CAC ¶ 245. See also *Kasky*, 27 Cal. 4th at 949.

Under the UCL's unfairness prong, Plaintiffs must show that the harm to themselves and

¹³ Google claims the federal Wiretap Act preempts all of Plaintiffs' privacy claims. D. Br. 30 n.15 (citing *In re Google Inc. St. View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011)). Not evaluating state law privacy, *Google St. View* only held that "the federal Wiretap Act preempts state wiretap statutory schemes." *Id.* at 1085. Google shows no conflict between Plaintiffs' privacy claims and the federal Wiretap Act, or how express, field, or conflict preemption might apply. See *Fellner v. Tri-Union Seafoods, L.L.C.*, 539 F.3d 237, 242-43 (3d. Cir. 2008).

the members of the proposed classes outweighs the utility of the Defendant's conduct. *Wahl v. Am. Sec. Ins. Co.*, No. C 08-00555 RS, 2010 WL 1881126, at *7 (N.D. Cal. May 10, 2010) (citing *Motors, Inc. v. Times Mirror Co.*, 102 Cal. App. 3d 735, 740 (1980)). Plaintiffs also satisfactorily allege liability under the UCL's unfairness prong by tethering Defendant's conduct to some "legislatively declared" policy. *Id.* (quoting *Cel-Tech Commc'ns., Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 185 (1999)). Plaintiffs show Defendant's actions are unfair because they contradict federal and state constitutional and statutory privacy principles, harm the Plaintiffs, and have no justification other than Google's desire for profits. CAC ¶ 246.¹⁴

Under the UCL's fraudulent prong, Plaintiffs need show only that "members of the public are likely to be deceived" by Google's schemes. *Stearns v. Ticketmaster Corp.*, 655 F.3d 1013, 1020 (9th Cir. 2011). Plaintiffs have clearly pleaded that deception. CAC ¶¶ 248-49.

Plaintiffs stating a UCL claim must plead an economic injury. Plaintiffs properly allege their actual damages from Defendants' conduct, detailing how their PII is valued by Internet users, Defendants, and the market. *See* CAC ¶¶ 49-67, 238-50. Defendant's argument that Plaintiffs "have not even attempted to show that they 'personally' suffered any loss of money or property," *see* D. Br. 33, ignores these allegations. Plaintiffs intend to provide expert testimony about the value of Plaintiffs' personal information. But, at this initial stage, Plaintiffs need not further quantify specific values associated with that personal information. *See* Sec. IV, *supra*. *See also Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 999 (N.D. Cal. 2006) ("at the pleading stage, general factual allegations of injury resulting from defendant's conduct may suffice").

¹⁴ *See also Marsh v. Zazoom Solutions, LLC*, No. C-11-05226-YGR, 2012 WL 6522749, at *18 (N.D. Cal. Dec. 13, 2012) (refusing motion to dismiss on UCL unfair prong, noting defendant "ignores the procedural posture of this case. At this juncture, the Court need only determine whether the allegations, which taken as true, state a plausible claim." (citing *Twombly*, 550 U.S. at 570)).

Plaintiffs have sufficiently pled the concrete, appreciable damages that establish standing and economic injury.

Google cites cases supposedly saying loss of PII is insufficient for UCL standing.¹⁵ See D. Br. 34. But in *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 811 (N.D. Cal. 2011), the court found that plaintiffs did have standing for their UCL claim. Google's other cases are distinguishable. In *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, MDL No. 11md2258 AJB (MDD), 2012 WL 4849054, at *15 (S.D. Cal. Oct. 11, 2012), the court found the heightened risk of identity theft, and alleged damage to the value of Plaintiffs' consoles too speculative. Here, Plaintiffs have pleaded a completed harm and the dollar value of their PII. *In re iPhone Application Litig.*, No. 11-md-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011), found that plaintiffs had "not adequately alleged *any* injury." Plaintiffs here have alleged violations of statutes providing injury-in-fact and compensable damages. Both *Ruiz v. Gap, Inc.*, No. 07-5739 SC, 2009 WL 250481 (N.D. Cal. Feb. 3, 2009) and *Thompson v. Home Depot, Inc.*, No. 07CV1058 IEG (WMc), 2007 WL 2746603 (Sept. 18, 2007) are pre-*Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) cases. *Krottner* concluded that "[i]f a plaintiff faces 'a credible threat of harm,' and that harm is both 'real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III." *Krottner*, 628 F.3d at 1143 (internal quotations and citations omitted).

F. COUNT VII - PLAINTIFFS STATE A CLAIM UNDER PENAL CODE § 502 (COMPREHENSIVE COMPUTER DATA ACCESS & FRAUD ACT)

By enacting § 502, the California legislature expanded the protection afforded to

¹⁵ *Del Vecchio I*, 2011 WL 6325910, neither discusses California's UCL nor sets a requirement that Plaintiffs had to try to sell their PII to succeed in their claim. *Id.* at *4 n.5.

individuals from unauthorized access to both their personal computers and individual data. Cal. Penal Code § 502(a). Under § 502(e)(1), anyone who suffers “damage or loss by reason of any violation of any provision of” § 502(c) may bring a civil action against the violator. Plaintiffs have asserted claims pursuant to §§ 502(c)(1)-(2), (6)-(7) which require allegations that Google accessed their computers “without permission.” Plaintiffs also assert a claim under § 502(c)(8), which requires allegations that Google introduced a “contaminant” into their computers.

1. The Complaint Alleges that Google Placed Cookies on the Plaintiff’s Computer Without Permission

The Complaint details the specific and intentional manner in which Google surreptitiously inserted an invisible form of its own creation, not authorized or created by the user, the sole purpose of which was to circumvent the default settings that would otherwise prevent placement of Google’s tracking cookies. CAC ¶¶ 68-126. Google’s insertion of hidden code into an invisible form to overcome the blocking settings renders untenable Google’s reliance on *In re iPhone Application Litig.*, 2011 WL 4403963. Not only was the form Google inserted not downloaded by users, unlike the applications in *iPhone*, but Google’s actions were necessary to overcome the barriers created by Safari’s default settings. CAC ¶¶ 68-72, 183-190.

2. The Complaint Alleges that Google’s Cookies are Contaminants

A “computer contaminant” is “any set of computer instructions that are designed to . . . transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.” § 502(b)(10). Google used embedded code and invisible forms without the owner’s intent or permission (CAC ¶¶ 1, 3,125), which were designed to transmit Plaintiffs’ information to Google. They are “contaminants.”

3. Damages and Losses

Plaintiffs have pleaded damages and losses. *See* CAC ¶¶ 262-264. Google’s reliance on

Nexsales Corp. v. Salebuild, Inc., No. C-11-3915 EMC, 2012 WL 216260 (N.D. Cal. Jan. 24, 2012), is misplaced. *Nexsales*'s holding turned on the absence of any "specific facts to support [plaintiff's] allegations." *Id.* at *3. Here, unlike *Nexsales*, Plaintiffs have specifically alleged the value of their PII and have pleaded the aforementioned damages and loss that include the diminution in value of their PII. *See* CAC ¶¶ 49-67.

G. COUNT VIII - PLAINTIFFS HAVE PLED A CAUSE OF ACTION UNDER THE CALIFORNIA WIRETAP ACT

California's Wiretap Act requires an interceptor to obtain the consent of *all* parties to a communication to avoid liability. More protective of privacy than its federal counterpart, California's act is not pre-empted. *See Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1024 (N.D. Cal. 2011) (no pre-emption where defendant "track[ed] individuals' internet habits and harness[ed] that data to sell and deliver targeted advertisements based on their web browsing history."); *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95 (Cal. 2006).¹⁶ Plaintiffs' CAC ¶¶ 1, 3, 125, 126 shows Google did not have any party's consent to the communication. *See supra*, Sec. V.A.2

Google argues it did not "willfully" intercept a protected communication. "Willfully" means "simply a purpose or willingness to commit the act... It does not require any intent to violate law, or to injure another, or to acquire any advantage." Cal. Pen. Code § 7.1. Google, the world's leading Internet advertising company, asks this Court to believe that it had no "purpose or willingness" to design and implement an unseen computer code (CAC ¶¶ 77, 78, 114), put it into an invisible iframe (*id.* ¶¶ 84, 114), to take advantage of a known browser loophole

¹⁶ *Sheppard v. Google*, No. 4:12-CV-04022, 2012 WL 6086867 (W.D. Ark. Dec. 6, 2012), rejected the same preemption argument Google makes here: "The only cases discussing the relationship between complete preemption and the ECPA have failed to find complete preemption." *Id.* at *4.

permitting cookie-setting (*id.* ¶ 105) that produced information (*id.* ¶109) and let Google compete against Facebook. *Id.* ¶¶ 100-104.. This risible claim presents a fact issue for discovery.

H. COUNT IX - PLAINTIFFS HAVE STATED A CLAIM UNDER THE CONSUMERS LEGAL REMEDIES ACT (“CLRA”)

Google argues that Plaintiffs fail to state a CLRA claim because Plaintiffs cannot allege (1) any “good or service” covered by the CLRA; (2) any “damage”; (3) any “purchase or lease”; or (4) that they provided a CLRA notice 30 days before filing an action for damages. None of these arguments have merit.

The CLRA protects consumers from “unfair methods of competition and unfair or deceptive acts or practices” in connection with the sale or lease of goods and services. Cal. Civ. Code § 1770. The statute “shall be liberally constructed and applied to promote its underlying purposes, which are to protect consumers against unfair and deceptive business practices...” Cal. Civ. Code § 1760. A “consumer” who suffers “any damage” as a result of any method, act, or practice prohibited by Section 1770 of the statute may assert a claim under the CLRA. Cal. Civ. Code § 1780(a).

Google argues that the CLRA does not apply to a “software activity,” but the cases Google cites for this proposition deal exclusively with software purchases. *See Ferrington v. McAfee, Inc.*, No. 10-cv-01455-LHK, 2010 WL 3910169, at *19 (N.D. Cal. Oct. 5, 2010); *See also In re iPhone Application Litig.*, 2011 WL 4403963, at *10; *compare Khoday v. Symantec Corp.*, 858 F. Supp. 2d 1004, 1011-12 (D. Minn. 2012) (denying motion to dismiss where law defining “service” was “conflicting” and finding product that made re-download of software more convenient qualified as a “service”).

Google’s advertising division sells a *service*, not software (*see* CAC ¶¶ 44, 278), even if

software is involved in that service. Google describes its advertising as “services.” *See* CAC ¶ 80. The CLRA reaches Google’s online advertising service. Cal. Civ. Code § 1761(b) (“‘Services’ means work, labor, and services for other than a commercial or business use, including services furnished in connection with the sale or repair of goods.”).

Plaintiffs have sufficiently pleaded damages, showing Google’s actions harm the value of their personal information. *See* CAC ¶¶ 49-67. “California courts have recognized that ‘damage’ in CLRA parlance is not synonymous with ‘actual damages,’ and may encompass ‘harms other than pecuniary damages.’” *Doe I, et al. v. AOL LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010) (citing *In re Steroid Hormone Prod. Cases*, 181 Cal.App.4th 145, 156 (2010)) (disclosure of plaintiffs’ personal information damages under CLRA); *see also Motschenbacher v. R. J. Reynolds Tobacco Co.*, 498 F.2d 821, 825 nn.10 & 11 (9th Cir 1974).

Google argues that Plaintiffs allege no “‘transaction’ that did or was intended to result in a ‘purchase or lease of goods or services.’” D. Br. 32. Plaintiffs’ use of websites to which Google supplied advertisements and correspondingly implemented cookies was a “transaction” under Civ. Code § 1761(e). That transaction was “intended to result or which results in the sale or lease of goods or services,” ultimately the sale of advertisements on websites and products. The consideration for using the Google services is the payment of personal information to Google. *See* CAC ¶¶ 49-67. This personal information is valuable to Google because, as Google admits (D. Br. 3) it allows Google to deliver targeted ads that are more valuable to advertisers. *See* CAC ¶¶ 44-45, 53-55. The exchange of Plaintiffs’ personal information in exchange for the use of Google’s services falls within the CLRA’s broad reach to protect consumers from “unfair and deceptive business practices.” Cal. Civ. Code § 1760.

Google’s next argument, that Plaintiffs did not provide the required written notice under

the CLRA, ignores the facts and misstates the law's requirements. Plaintiff Lourdes Villegas complied with § 1782's requirements. *See* CAC ¶ 283 (Villegas's initial complaint only sought injunctive relief and she gave Google written letter notice). Google cites Cal. Civ. Code § 1782, which states that notice of a CLRA violation must be given "[t]hirty days or more prior to the commencement of an action for damages." Google ignores the qualifier on "an action for damages," erroneously arguing that Plaintiff was required to give 30-days' notice before filing a complaint that did not seek CLRA damages. Civil Code section 1782(d), which Google seemingly ignores, shows Plaintiff Villegas acted properly and Google's arguments fail:

An action for injunctive relief brought under the specific provisions of Section 1770 may be commenced without compliance with subdivision (a). Not less than 30 days after the *commencement of an action for injunctive relief*, and after compliance with subdivision (a), the consumer may amend his or her complaint without leave of court to include a request for damages. The appropriate provisions of subdivision (b) or (c) shall be applicable if the complaint for injunctive relief is amended to request damages.

Cal. Civ. Code § 1782(d). *See, e.g., Stickrath v. Globalstar, Inc.*, 527 F. Supp. 2d 992, 1001 (approving course of conduct similar to Plaintiffs' and distinguishing different cases).

VI. CONCLUSION

Google's Motion to Dismiss should be denied on all counts of Plaintiffs' Complaint.

Dated: March 29, 2013

KEEFE BARTELS, LLC

/s/ Stephen G. Grygiel
Stephen G. Grygiel (Del Bar No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefbartels.com

Executive Committee Member

**BARTIMUS, FRICKLETON,
ROBERTSON & GORNY, P.C.**

/s/ James P. Frickleton
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertson, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

**EICHEN, CRUTCHLOW, ZASLOW &
MCELROY LLP**

/s/ Barry Eichen
Barry R. Eichen
40 Ethel Road
Edison, NJ 08817
Tel: 732-777-0100
beichen@njadvocates.com
Plaintiffs' Steering Committee Member

Respectfully submitted,

STRANGE & CARPENTER

/s/ Brian Russell Strange
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

STEWARTS LAW US LLP

/s/ Ralph N. Sianni
Ralph N. Sianni (Del Bar No. 4151)
Michele S. Carino (Del Bar. No. 5576)
Lydia E. York (Del Bar No. 5584)
I.M. Pei Building
1105 North Market Street, Suite 2000
Wilmington, DE 19801
Tel: 302-298-1200
rsianni@stewartslaw.com

*Plaintiffs' Steering Committee Member and
Liaison Counsel*

SEEGER WEISS LLP

/s/ Jonathan Shub
Jonathan Shub
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Tel: 215-564-2300
jshub@seegerweiss.com
*Counsel for Plaintiff Lynne Krause and
Plaintiffs' Steering Committee Member*

MURPHY P.A.

/s/ William H. Murphy, Jr.

William H. Murphy, Jr.
One South Street, Suite 2300
Baltimore, MD 21202
Tel: 410-539-6500
billy.murphy@murphypa.com

Plaintiffs' Steering Committee Member

BARNES & ASSOCIATES

/s/ Jay Barnes

Jay Barnes
219 East Dunklin Street
Jefferson City, MO 65101
Tel: 573-634-8884
Jaybarnes5@gmail.com

Plaintiffs' Steering Committee Member

BRYANT LAW CENTER, PSC

/s/ Mark Bryant

Mark Bryant
601 Washington Street
P.O. Box 1876
Paducah, KY 42002-1876
Tel: 270-442-1422
mark.bryant@bryantpsc.com

*Counsel for Plaintiff William G. Gourley
and Plaintiffs' Steering Committee Member*